Single Connect Kron

Datasheet

DATA ACCESS MANAGER & DYNAMIC DATA MASKING (DDM)

Organizations rely heavily on data security. Regardless of the industry (financial, insurance, telecom, pharma, etc.) or data type (product, employee, customer, financial, medical), **organizations recognize the need to secure and effectively monitor their sensitive data.**

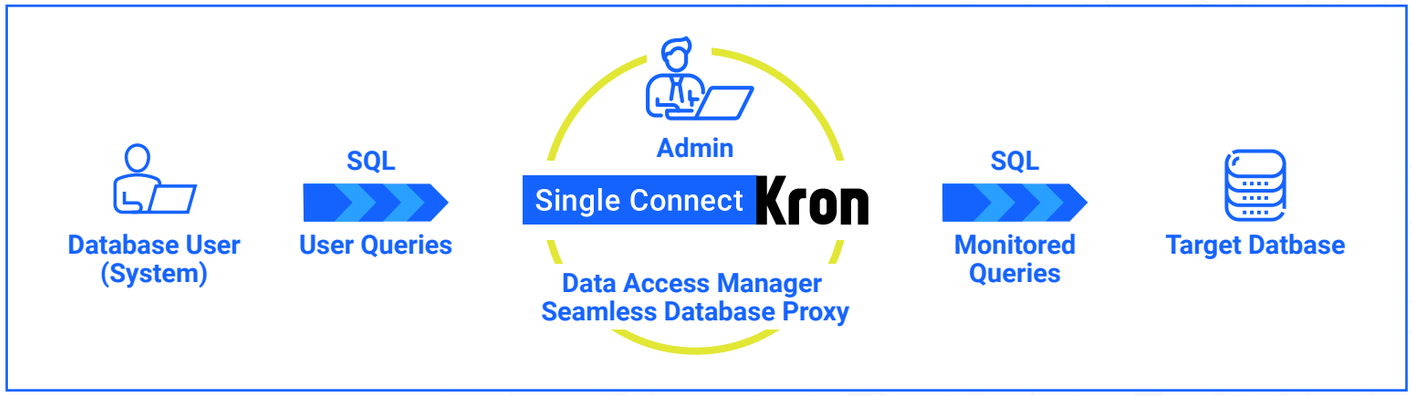
Data breaches or data loss may affect stakeholders negatively and may lead to the loss of stock prices, customer dissatisfaction and even **financial crisis**. Ignoring the compliance to GDPR or the regulations in the related countries cannot protect companies from the data breaches. Therefore, organizations need to reduce the effect of breaches by integrating **data access or data masking** solutions to avoid fines and to comply with regulations.

In this solution brief, you will learn about Data Access Manager capabilities provided by Kron Single Connect, including the following:

- Single Connect comprehensively logs all privileged session database connections and activities that may generate data breaches and impact business continuity.
- Single Connect efficiently and centrally secures and controls privileged access to databases and provides users a dedicated access to the information that is assigned to them, not any other information.

In this solution brief, you will learn about Data Access Manager capabilities provided by Kron Single Connect, including the following:

Single Connect Data Access Manager provides session logging functionality to database admins. All database queries can be logged for security and compliance purposes. The user experience is unchanged as they continue to use their own database client. The client can communicate with Single Connect Data Access Manager through the standard protocol used by the database.



Database admins can control logging as well as user permissions to execute SQL commands, by employing policy enforcement and database masking as preventive actions.

Single Connect Kron

Datasheet

Policy and Access Management

Database admins can control user permissions to run SQL queries by establishing rules or policies that comply with the established security requirements. **Single Connect Data Access Manager policy enforcement** can be accomplished in four ways:

1. **Blacklist and whitelist**
2. **Time-based restrictions**
3. **Maintenance mode restrictions**
4. **Context based restrictions**

Dynamic Data Masking

Data masking technology is aimed at preventing the abuse of sensitive/confidential data by giving users fictitious (yet realistic) or **hidden data**, instead of real and sensitive data.

Data masking targets the misuse of data at rest, typically in **nonproduction databases** (static data masking), and data in transition, typically in production databases (dynamic data masking).

Dynamic Data Masking is necessary, especially for application testing use cases that require representative and coherent data. **Dynamic data masking (DDM) limits sensitive data exposure by masking it to non-privileged users.**

ORIGINAL DATA		
Name	**Phone**	**Birth Date**
John Doe	511-336-4455	11.4.1986
Adam Smith	511-472-1314	2.2.1967

MASKED DATA		
Name	**Phone**	**Birth Date**
John Doe	511-111-1111	1.2.1987
Adam Smith	511-123-4567	10.11.1966

DDM can also be configured to hide sensitive data in the database query result sets over designated **database fields, while the data in the database remains unchanged**. DDM supports following masking rules; Redaction/Nulling, Shuffling, Blurring, Tokenization, Substitution and other Custom rules defined by regular expressions.

ORIGINAL DATA			
Name	**Phone**	**Birth Date**	**Credit Card**
John Doe	511-336-4455	11.4.1986	1111 2222 3333 4444
Adam Smith	511-472-1314	2.2.1967	555-6666-7777-8888

MASKED DATA			
Name	**Phone**	**Birth Date**	**Credit Card**
John Doe	511-111-1111	1.2.1987	1111 2222 3333 XXXX
Adam Smith	511-123-4567	10.11.1966	555-6666-7777-XXXX

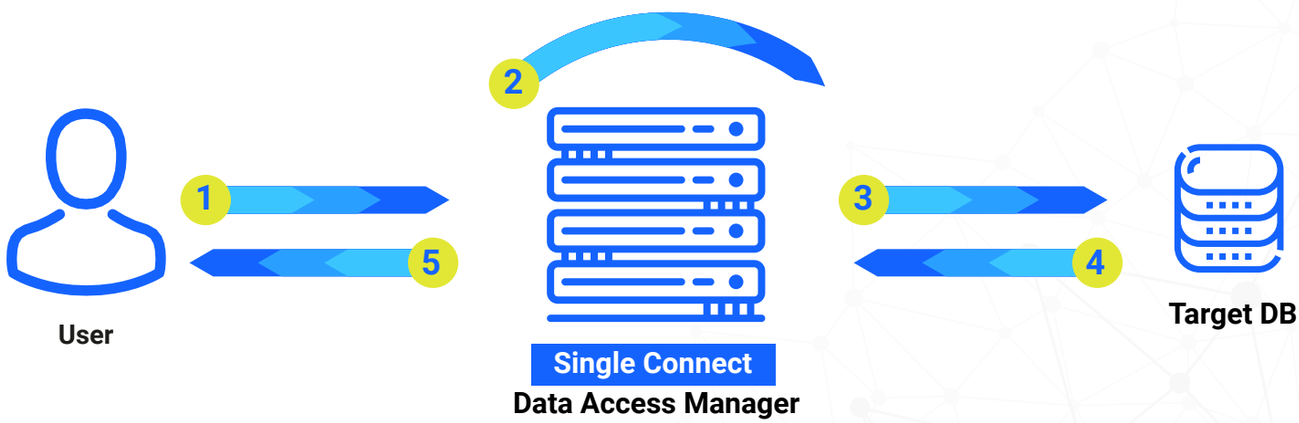
Single Connect Kron

Datasheet

HOW IT WORKS

Data Access Manager uses a man-in-the-middle proxy to control numerous kinds of databases - e.g. Cassandra, Hive, IBM DB2, Microsoft SQL Server, MySQL, Oracle and Teradata, among the others from a central point. Requests to databases and queries prevented over proxy component that authorized by Dynamic Data Masking product for the seized SQLs before. **The conjunction of Data Access Management and Dynamic Data Masking achieves data security protection within the data layer itself and carries out solid protection for database security.**

- **Database activities monitored by the proxy to permit any action that needs to be done.**
- **Data Access Manager separates out records and shows database query results in accordance with the authorized users and logs all data access sessions.**
- **Dynamic Data Masking prepares or masks individual piece of information inside the filtered data set. DDM engine controls exactly who should gain access to what, where, when, why and how; down to the level of individual cells in database queries.**



Step 1: User runs query.

Step 2: The query is logged and then re-written based on the policy rule. If DDM is activated, (2A) query passes to DDM module and enhanced masking rules are executed. (2B) Masked query returns to Data Access Manager.

Step 3: Manipulated query is forwarded to target DB.

Step 4: Target DB returns the result of query to Single Connect's Data Access Manager.

Step 5: Single Connect's Data Access Manager forwards the filtered results to the user.

Single Connect Kron

Datasheet

BENEFITS

Single point of access control management for database layer.

All queries are logged indisputably. Users **authenticate** with their own credentials even if there is no such DB user, so the real user running a **query is known and logged.**

Discovers **sensitive data** such as credit card or personal ID numbers residing in Database and **Big Data** servers.

Sensitive data can be manipulated and delivered to **applications or users** in such a manner that it is no longer sensitive, but still coherent and usable.

Policies (DB masking rules) can easily and **instantly be assigned** to users, application accounts and/or groups and roles.

Minimizes the r**isk of disclosure** for data in progress

Accounts can be **time-limited** (hours of day, day of week, etc.).

Has no performance degradation impact on target Databases.

Users are not required to use a proprietary **database** client and can continue using familiar tools (i.e. Toad, etc.). Authorization can be made without any interference.

Eliminates weak and **non-expiry passwords**. Disables inactive accounts.